REMARKS

The Office Action took a relatively broad interpretation of the *Sabin et al.* (U.S. Patent No. 6,026,421) in rejecting Claims 1-18 under 35 U.S.C. § 102.

In order to meet the requirements of 37 C.F.R. § 1.116, applicant has redrafted dependent Claim 10 into an independent Claim 19, and Claims 11-14 now depend from this claim. Thus, no new issues are presented, but rather the patentability of the previously rejected dependent Claim 10 is now at issue. It is requested this amendment be entered as meeting the requirements of § 1.116.

Sabin et al. is directed to a system for performing arithmetic computations involving large integers such as may be demanded in cryptography for RSA and DSA schemes. As set forth in Column 2, the *Sabin et al.* reference is directed to an observation that both multiprecision multiplication and modular reduction can be rapidly calculated on a relatively economical computing device by carrying out the following operation:

$$Z \leftarrow Z \pm (X * Y)$$

Sabin et al. taught the use of a coprocessor to complement a computing device and further taught various applications of memory units, including a dual ported RAM apparatus, with a single write-port and a single read-port. See Column 14, Lines 29-36.

The present invention also addresses an encryption system, and more particularly, sought to optimize the implementation of elliptic curve cryptology (ECC).

The implementation of a high security ECC that can be executed with a smaller bit key than in RSA encryption requires the capability of increasing the number of calculations and the ability of a coprocessor to handle the multi-word arithmetic required for ECC. Additionally, the present invention attempts to use a relatively small-scale circuit and an implementation method of enabling the control circuit to eliminate certain calculation steps. For example, calculating the lower words of an integer A shown in Figure 15, these features provide a significant impact in that the arithmetic unit can run at a higher speed while the size of memory required for computation is reduced. Thereby the advantages of a higher security can be applied in more economical applications.

Referring to the newly drafted Claim 19, the arithmetic unit adds one piece of one-word data containing all ones to the piece of intermediate data D and the integer AA. Reference can be made, for example, to Figure 15 of our present application and to the teachings at Page 42, Line 14, through Page 44, Line 21.

More specifically, the following teaching is found on Page 43, Line 10, through Page 44, Line 21:

> Therefore, in step 2, the required calculation is executed focusing only on the upper five words of the calculation result. However, since a carry from the sixth word (the sixth from the most significant digit, other words referred to below also being so defined) to the fifth word is considered when computing (BxP+A), the multiplication of integers B and P and the addition of integer A are performed on the upper six words of the integer.
>
> Furthermore, a word containing all ones is also added when performing additions for the sixth word. This enables any carry propagated to the fifth word from the seventh word via the sixth word to be considered when computing (BxP+A). Since it has been ascertained, as described above, that the sixth word for the calculation (BxP+A) must be '0', the carry from the seventh word only needs to be considered if the result of adding the data c_0 and the data a_4 not '0'. If the result of adding the data c_0 and the data a_4 is '0', there is no need to check for a carry, as any carry can be propagated simply by adding the integer E (e_0).
>
> Note that incorporating the addition of the data e_0, having ones in all its bit positions, in the addition of the data c_0 and the data a_4 is equivalent to performing one of the following processing (1) to (4).

> (1) When the addition result of data c_0 and data a_4 is '0', and the carry is also '0', a carry '0' is added to the computed data m_0 (c_1+a_5).
>
> (2) When the addition result of data c_0 and data a_4 is '0', but the carry is '1', a carry '1' is added to the computed data m_0 (c_1+a_5).
>
> (3) When the addition result of data c_0 and data a_4 is not '0', but the carry is '0', a carry '1' is added to the computed data m_0 (c_1+a_5).
>
> (4) When the addition result of data c_0 and data a_4 is not '0', and the carry is '1', a carry '2' is added to the computed data m_0 (c1+a_5).
>
> (Underline added.)

As can be appreciated, recent increases in computing power increase the necessity to realize economical encryption schemes for implementation in electronic commerce. The ability to provide more efficient and economical hardware and computation requirements is constantly being sought by a large number of highly skilled engineers and computer scientists. The patentability of our invention must be considered in light of this background and the advantages that can be realized over the teachings in the *Sabin et al.* reference.

Here, the "piece of intermediate data D", "integer AA", and "a piece of one-word data containing all ones" recited in Claim 19 correspond to the "integer C", "*upper* six words of the integer A", and "the integer E (e_0)" in our specification.

As described above, owing to the addition by the arithmetic unit of a piece of one-word data containing all ones to the piece of intermediate data D and the integer AA, it is no longer required to calculate the lower words of the integer A (the lower words other than the integer AA, which is the upper (n+1) words of the integer A). This significant effect leads to an arithmetic unit that runs at a higher speed and the memory required for the computation is reduced.

The *Sabin et al.* reference primarily discloses a technique for performing multiplication and modular reduction of large integers. Figure 3 of *Sabin et al.* shows four large integer units (LIU). Each word of a large integer is associated with one of the four LIU and the word is computed by an associated LIU. That is, *Sabin et al.* teaches using a plurality of LIUs to perform computations on large integer words. With this structure, in order to compute an integer having longer word-length, the circuitry needs to be inevitably larger.

Sabin et al. does not disclose or imply the patentable feature of Claim 19, where "the arithmetic unit adds a piece of one-word data containing all ones to the piece of intermediate data D and the integer AA".

Even applying the teaching of *Sabin et al.* to the calculating procedure quoted above from the present application, the calculation M = (B x P + A)/R (the step S204 shown in Figure 4) cannot be performed without the addition of the lower words of the integer A.

On the contrary, the invention recited in Claim 19 of the present invention makes it unnecessary to carry out the addition of the lower words of the integer A. In light of the above, it is respectfully submitted that the invention recited in Claim 19 is patentable over *Sabin et al.* Consequently, the inventions recited in dependent Claims 11-14 are also in condition for allowance.

It is believed that the case is now in condition for allowance, and an early notification of the same is requested.

If the Examiner believes that a telephone interview will help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 22, 2005.

By: Sharon Farnus

Sharon Farnus

Signature

Dated: April 22, 2005

Very truly yours,

SNELL & WILMER L.L.P.

Joseph W. Price
Registration No. 25,124
1920 Main Street, Suite 1200
Irvine, California 92614-7230
Telephone: (949) 253-4920